# 无线体域网中节点认证方案研究 *

朱　斌，朱　帅

(重庆大学 通信工程学院，重庆 400030)

**摘　要：** 针对无线体域网中节点身份认证问题，在传统椭圆曲线签名算法的基础上，提出了一种新的在线\离线椭圆曲线签名方案。该方案在未确定签名消息之前进行离线签名，在确定要加密的消息和身份私钥之后进行在线签名。对该方案进行了安全性分析，证明了其具有正确性、不可伪造、不可否认、抵御重放攻击、轻量级的优点，同时通过运算量的对比分析，表明该方案由于取消了求逆运算，具有较大的计算优势。

**关键词：** 无线体域网；身份认证；在线/离线椭圆曲线签名

**中图分类号：** TP302　　doi: 10.3969/j.issn.1001-3695.2018.03.0172

## Research on node authentication scheme in wireless body area networks

Zhu Bin, Zhu Shuai

(*College of Communication Engineering*, *Chongqing University*, *Chongqing* 400030, *China*)

**Abstract:** Based on traditional elliptic curve digital signature scheme, this paper proposed a new online/offline elliptic curve digital signature scheme to solve the node authentication problem in wireless body area networks. In this scheme, offline signature would be done before the signatures ware confirmed, and online signature would be done after the information and private key ware confirmed. It made the security analysis to prove that the scheme has validity, anti-falsification, non-repudiation, avoided replay attack and lightweight. Compared with calculation, this scheme doesn’t need the inverse operation, which shows the advantages of calculation.

**Key words:** wireless body area network; authentication; online/offline elliptic curve digital signature



## 0　引言

无线体域网[1]是由一些放置在人体表面或者植入人体内部的传感器以及一些可移动终端所组成的以人体为中心的网络。随着人们对无线体域网的深入研究，无线体域网的安全问题越来越受到人们的重视，身份认证在信息安全中具有特殊的作用，大多数情况下是与密钥协商等方法结合起来作为一个大的整体信息保护方案被提出。身份认证是身份识别(identification)和身份认证(authentication)的统称，是用来验明用户是否具备所请求资源的使用和存储权，即验证查核用户身份的过程。身份认证中最为关键的是可以准确无误地将对方辨认出来。在体域网系统当中，人们需要的是对节点之间的身份进行相互的认证。节点间的身份认证是体域网生理信息安全传输的首要保障，一旦节点间的身份认证体系被攻破，那么整个传输系统的所有安全措施便将形同虚设。

因此设计安全的认证协议来保障体域网数据传输的安全。近年来，椭圆曲线密码机制作为很重要的一种且近来受到广大研究者的热捧，有其衍生出的椭圆曲线签名算法[2]具有广阔的应用前景。它由 Vanstone 在 1992 年对 NIST 的 DSS 回应的建议中提出来[3]。但是到 1998 年才被接纳为 ISO（国际标准化组织）接纳为标准（ISO1488-3）。在国外，主要是针对一些具体应用的椭圆曲线签名方案的研究[4, 5]；在国内，有 ECDSA 的硬件 VLSI 设计[6]、基于 FPGA 的签名芯片的开发[7]等。

## 1　基于椭圆曲线的签名方案

椭圆曲线有限群上的数字签名方案（如 Okamoto、ELGamal、DSA、Schnorr 等）均基于的是离散对数难题[8]。在讨论分析中，对椭圆曲线签名方案的基本参数有如下约定：

设椭圆曲线 $E_p(a,b)$ 是定义在有限域 $F_q$ 上的一条安全椭圆曲线，在椭圆曲线上随机的选取一个点作为基点 P，设 r 是 n 的大数因子，$H(\cdot)$ 为单向 hash 函数。这样基于椭圆曲线离散对数问题的数字签名方案（elliptic curve digtial signature）可描述如下。

### 1.1　初始化过程

完成参数初始化之后，需要分发密钥。在人们的环境中，

**收稿日期：** 2018-03-03；**修回日期：** 2018-04-19　　**基金项目：** 国家自然科学基金资助项目（61571069）

**作者简介：** 朱斌（1981-），男，重庆忠县人，副教授，博士（后），主要研究方向为网络安全、人工智能（zhubin@cqu.edu.cn）；朱帅（1992-），男，山西五台县人，硕士研究生，主要研究方向为体域网中的网络安全.

节点 A、B 的基本密钥对是根据算法 $Q = dP$ 产生的，其私钥 $d_A, d_B$，公钥 $Q_A, Q_B$ 作为公开参数被公开允许任何节点访问，待签名的消息为 $m$，签名值为 $S$。

### 1.2　签名过程

这里本文以汇聚节点 B 验证采集节点 A 的身份作为示例。具体签名步骤如下：

a)节点 A 计算消息 m 的摘要值 $H(m)$；

b)节点 A 随机选择一个大整数 $k \in [1, n-1]$，计算 $Q = k \times P = (Q_x, Q_y)$；

c)这里设签名方程 $Q_x = [S - H(m) \times k] \times d_A$，由该签名方程求解可得签名 S。

$$S = H(m) \times k + Q_x \times d_A^{-1} \tag{1}$$

d)节点 A 将 $(Q, S)$ 作为消息 $m$ 的数字签名发送给节点 B。

### 1.3　认证过程

当接收者节点 B 收到消息 $m$ 和数字签名（Q, S）后，可以按照以下步骤对待核实的消息签名进行认证：

a)节点 B 用消息摘要算法计算消息 $m$ 的摘要值 $H(m)$；

b)节点 B 查询节点 A 的公钥 $Q_A$，将收到的签名分解出来得到 $Q$、$S$ 和 $Q_x$；

c)将 $S$、$H(m)$ 和 $Q_x$ 代入验证方程：

$$H(m) \times Q = S \times P - Q_x \times Q_A \tag{2}$$

验证其是否成立。若成立，则接受该节点并记录相关信息；否则拒接该节点的消息。

ECDS 数字签名方案的工作过程如图 1 所示。

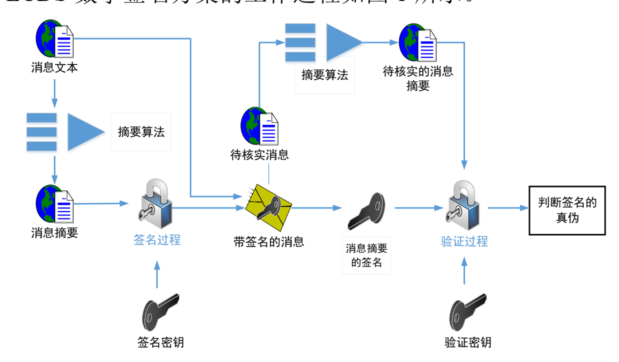



图 1　ECDS 方案的工作过程

### 1.4　安全性分析

上述数字签名方案的正确性证明如下：

$$\begin{aligned} S \times P - Q_x \times Q_A &= \{H(m) \times k + Q_x \times d_A\} \times P - Q_x \times Q_A \\ &= H(m) \times k \times P + Q_x \times d_A \times P - Q_x \times Q_A \\ &= H(m) \times Q + Q_x \times Q_A - Q_x \times Q_A \\ &= H(m) \times Q \end{aligned}$$

所以，ECDS 数字签名方案是正确的。该方案中节点 A 和 B 分别使用自己的私钥进行了信息的加密，非法的攻击者只有获取了私钥才能进行攻击，而私钥的获取是基于椭圆曲线离散对数的一个难题。除此之外，攻击者无法推测出采集端点的口令原文，因而也无法通过认证过程。因此该方案具有一定的安全性保护。另外，随机数的选取不仅保证了节点 A 和 B 在通信前的请求和认证，同时有效防止了重放攻击对用户私钥进行破解。

但是该方案具有以下的不可靠性：

a)在以上的数字签名方案中，发送节点是不能否认自己曾经发送过得消息的，而对接收节点却没有任何约束，这样就可能存在两种情况：

(a)接收节点已经阅读了消息，事后却否认自己曾接受过该消息。例如接受节点接收并阅读到了一条消息，但是却将其丢失并否认自己曾接收过该消息。

(b)接收节点故意拖延阅读时间，以作出对自己更有利的决定。例如发送节点在上午 10 点之前将信息发送给接收节点，而接收节点此时因为某些原因没有实时处理，10 点以后才开始处理信息，结果事后反而指责发送节点并未实时发送签名信息从而完成认证。

收方不可否认数字签名方案就是为了解决这些问题而提出来的。在这一方案中，没有签名者的合作，接收方就无法验证签名，这使得发送节点的利益得到某种程度上的保护。而当涉及到与时间相关的通信时，还需要引入时间戳的概念，记录双方通信的时候和阅读情况，以确定责任归属。但是时间戳对系统要求比较高，需要很强的时钟同步，无线体域网中的节点能力有限，所以时间戳方法并不适用，可以采用随机数来保证消息的新鲜性。

b)在该签名 S 的计算中，不仅有数乘运算和加法运算，同时还有求逆运算，对于大整数求逆是比较耗时的一种运算，使用扩展的欧几里得算法平均也需完成 $0.843\log_2 n + 1.47$ 次除法。因此若能减少求逆运算，则可以提高签名和验证的计算量，从而提高系统速度。

轻量级的方案对于体域网而言是相当重要的，因为体域网网络环境以及体域网中节点的特殊性，尤其对其中只有很小的存储量和有限的计算能力的节点芯片而言，所以除了将求逆运算化为普通数乘运算的同时，引入在线/离线技术将具有很大的计算优势。

## 2　在线/离线椭圆曲线签名方案

### 2.1　在线/离线签名系统

在线/离线签名系统中，签名运算被分解成两个过程：第一个过程被称为离线签名，即在未确定签名消息之前所做的签名运算；第二个过程被称为在线签名，即在确定要加密的消息和身份私钥之后所做的签名计算。该签名技术使得在线阶段消耗较少的资源，而离线阶段进行大部分的计算。这种签名方案对于计算能力有限的设备（尤其是体域网中的节点设备）来说是非常有用的。

在线/离线签名（OS）系统包括 KeyGen、OffSign、OnSign、Ver 四种算法，分别是密钥生成、离线签名、在线签名及签名验证。

KeyGen：这是一种概率多项式时间算法。该算法有 PKG 执

行。输入一个安全参数 $1^k$，输入用户主参数 params、私钥 SK 和对应的公钥 PK。

OffSign：这是一种由签名者执行的概率多项式时间算法。输入用户主参数 params、私钥 SK 和对应的公钥 PK。

OnSign：同样这也是由签名者执行的概率多项式时间算法。输入用户主参数 params、私钥 SK、待签消息 M 和状态信息 St，输入在线签名 $\sum^{on}$，得到最终关于消息 M 的签名为 $\sigma_m=(\sum^{off},\sum^{on})$。

Ver：这是一种由验证者执行的多项式时间算法，不同的是该多项式时间算法是确定的。输入用户主参数 params、被签消息 M、签名 $\sigma_m$ 和公钥 PK。如果签名是有效的，输出 accept；否则输出 reject 拒绝该签名。

现在构造一个新的在线/离线签名方案，该方案是基于上一节所提出的椭圆曲线的签名方案。原始的椭圆曲线签名（ECDS）方案并不能直接实现在线/离线签名，ECDS 改成 OS 的一般方法是借助变色龙哈希来实现。安全的变色哈希实现可以实现任意可证明安全的签名方案到 OS 签名的一般构造[9]，而这里的椭圆曲线签名方案已经有相当多的文献证明了其安全性。变色龙哈希如下所述。

设 G 是一个 p 阶循环群而且 g 是群 G 的一个生成元。随机地选择一个值 y 来自 $Z_p^*$，同时随机选择一个群 G 的生成元 g，并且有 $g_2=g^y$。那么验证公钥是 $(g,g_2)$，私钥是 y。变色龙哈希输入元素是一组来自 $Z_p$ 的元素 $(m,r)$，输出元素是一个来自 G 的元素。具体的变色龙哈希定义如下：

$$H(m,r)=g^r g_2^m \tag{3}$$

给一个新的 $m'\neq m$，使得 $r'=(m-m')y+r$，从而有 $H(m',r')=H(m,r)$。因此，只要变色龙哈希具有安全性且攻击者仅仅获取到 $(m,r,H(m,r))$，那么任何攻击者都不能够在多项式时间内找到一组新的 $(m',r')$，以至于在 $m'\neq m$ 时，$H(m',r')=H(m,r)$ 是成立的。

### 2.2　在线/离线椭圆曲线签名方案

有了变色龙哈希的存在，就可以进行适当的改动，便有了如下的在线/离线椭圆曲线签名（ECDSOS）方案。此方案包含五个阶段，分别是系统初始化阶段、密钥生成阶段、离线签名阶段、在线签名阶段和签名认证阶段。各阶段流程如下：

a)系统初始化阶段。

初始化主要是完成参数的初始化以及系统的准备工作。设 $E_p(a,b)$ 是定义在有限域 $F_q$ 上的一条安全椭圆曲线，该曲线 $E_p(a,b)$ 上的有理点构成的群的阶能够被一个大的素数 n 整除。在曲线上随机选取一个点作为基点 P，以 P 作为生成元对椭圆曲线 $E_p(a,b)$ 上的加法运算构成了一个循环子群<P>，其阶为 n，并且满足条件 $nP=O$，$O$ 表示一个无穷远点。基点 P 作为公共信息被公开。设 $(1^\ell)\rightarrow(Q,G_1,G_2,e)$，其中 $G_1,G_2$ 都是 p 阶乘法循环群。同时设单向 $Hash$ 函数 $H:\{0,1\}^*\rightarrow G_2$。每个参与身份认证的节点都有一个 MAC 地址和一个唯一的身份标志符 ID，这些信息代表了需要认证节点的身份信息。节点 A 为签名者，B 是对节点 A 进行身份认证的节点。M 是一个消息空间，表示原生理信息，$M=\{0,1\}^*$，$M_w$ 表示节点 A 的签名许可凭证，其中包含节点 A 的身份信息（MAC 和 ID 信息）、公钥信息等内容。

b)密钥生成阶段。

节点 A 随机选择 $d_A\in Z_p^*$ 作为私钥，椭圆基点为 P，计算公钥 $Q_A=d_AP=(Q_{Ax},Q_{Ay})$。存储密钥 $d_A$ 和公布公钥 $(G_1,G_2,H,P,Q_A)$。

c)离线签名阶段。

节点 A 随机选择两个整数 $m,r\in Z_p$，并计算 $u=Q_A\times m+P\times r$。存储状态信息 $(r,m)$，计算离线签名 $\sigma'=H(u)$，并输入离散签名 $\sigma'$。

d)在线签名阶段。

节点 A 恢复出状态信息 $m,r$。对于待签的生理信息，首先计算生理信息 M 的摘要值 $H(M)$，然后计算消息 M 的在线签名 $r'$。

$$r'=\{m-H(M)\}d_A+r \tag{4}$$

而后加上属于节点 A 的签名许可凭证 $M_w$，最后关于消息 M 的完整签名是 $\sigma_M=(\sigma',r',M_w)$，将其发送给节点 B，同时使用混合加密算法中的共享密钥加密传输状态信息 $(r,m)$ 给节点 B。

e)签名认证阶段。

节点 B 在接收节点 A 发来的签名信息 $\sigma_M=(\sigma',r',M_w)$ 之后，这里假设是 $\sigma_M$ 一个有效地关于 M 的签名，输入验证公钥 $(G_1,G_2,H,P,Q_A)$，利用已接受到的生理消息 M，用消息摘要算法计算消息 M 的摘要值 $H(M)$，计算 $u'=Q_A\times H(M)+P\times r'$，而后验证方程 $H(u')=\sigma'$ 是否成立。如果 $\sigma'$ 是关于 u'的一个有效签名，即该验证方程成立，那么节点 B 完成对节点 A 的身份认证；否则节点 A 未通过节点 B 的身份认证。

同时节点 B 将状态信息解密出来计算 $R=r+m$ 后，同样用节点 A，B 的共享密钥发回给节点 A。

## 3　安全性分析

1)正确性分析

若签名合法，$u'=Q_A\times H(M)+P\times r'$，节点 B 在接收节点 A 发来的签名消息后（该签名消息包含离线签名 $\sigma'$、在线签名 $r'$ 以及节点 A 的签名许可凭证 $M_w$），对生理信息 M 的摘要值 $H(M)$ 以及在线签名 $r'$ 做以上的相关运算，因为存在如下的等式成立：

$$\begin{aligned}u'&=Q_A\times H(M)+P\times r'\\&=Q_A\times H(M)+m\times Q_A-H(M)\times Q_A+P\times r\\&=m\times Q_A+P\times r\\&=u\end{aligned}$$

显然有 $H(u')=H(u)=\sigma'$ 成立。那么节点 B 通过收到的签名消息做相关运算后求解出 $H(u')$ 与收到的离线签名 $\sigma'$ 做比较。若相等，则可认为签名有效，节点 B 完成对节点 A 的身

份认证；若不相等，则表示签名无效，节点 A 无法通过节点 B 的身份认证。

2)不可伪造性

攻击者 C 要破解签名者节点 A 的签名密钥 $d_A$，需要通过求解方程 $r'=\{m-H(M)\}d_A+r$ 获取。在第 2 章混合加密算法的保证下，消息 M 是不会有任何泄露的。方程中有 $m$，$H(M)$，$r$ 作为未知数，并不能求出签名密钥 $d_A$；若攻击者 C 截获签名 $\sigma_M=(\sigma',r',M_w)$，通过 $\sigma'$ 获取 $u$ 并不可能，因为这是一个单项散列函数的逆向求法，是不可能实现的，攻击者 C 可以通过暴力手段获取到状态信息 $(r,m)$，攻击者 C 获得一对 $(\sigma',r')$，但是方程中始终有两个未知参数 $d_A$ 和 $H(M)$。若获得多对有效签名 $(\sigma_1',r_1'),(\sigma_2',r_2'),\cdots,(\sigma_n',r_n')$，但是每次序列产生时 $H(M)$ 都是由生理信息生成的，生理信息的伪随机性使得求解 $d_A$ 的方程组没增加一个同时也会增加一个未知数 $H(M)$，并且状态信息也是每次都会变化，故也没有办法在多项式时间内解出 $d_A$；若已知 $Q_A$ 求 $d_A$，则困难性等价于求椭圆曲线离散对数问题，因此是不行的。

有了以上对于私钥 $d_A$ 的不可求解性，那么攻击者 C 欲产生“合法”签名。他需要通过选择合适 $m,r$ 构造 $\sigma'$ 以及合适的 $d_A$ 和 $H(M)$ 来构造 $r'$。并且本文的方案是由变色龙哈希演变而来，同样变色龙哈希在多项式时间内是找不到一组新的 $(m',r')$ 以至于在 $m'\neq m$ 时，$H(m',r')=H(m,r)$ 是成立的。由前面的分析 $d_A$ 的不可求解性和 $H(M)$ 是绝对安全性，以及借鉴的变色龙哈希可知，该方案是满足不可伪造性的。

3)不可否认性

签名验证时，首先需要验证 $u'=Q_A\times H(M)+P\times r'$ 的正确性。显然，节点 A 的公钥 $Q_A$ 参与验算，否则验证不通过，且 $r'=\{m-H(M)\}d_A+r$，由不可伪造性分析可知，节点 A 的私钥是随机生成的，攻击者是无法伪造同样的私钥的。这是因为私钥是不公开的，想要通过公钥获取私钥是不可能实现的，因为他将面临 ECDLP。因此，所有签名者的私钥和公钥都参与了签名的构造，当签名完成时，也就表明所有人参与了签名的过程，满足不可否认性。而对于节点 B 而言，因为加入了随机数的信息，一旦节点 B 处理了签名消息，将会有一个相应的随机数返回给节点 A，节点 B 也就无法抵赖，满足不可否认性。

4)抵御重放攻击

在签名方案中，当攻击者使用前面的签名信息或者之前发送过的签名信息再次发送给接收验证节点时，验证节点就无法判断该签名消息是否是新鲜的，攻击者就可以进行重放攻击。而一般情况下都是通过时间戳来解决这个问题，但是时间戳对系统要求相对而言是较高的，需要极强的时钟同步，无线体域网中节点能力有限，时间戳方法并不太适用。因此这里使用的是随机数来保证消息的新鲜性，使得节点 A，B 形成询问——应答模式，即发送方节点选择一个随机数，利用双方节点的共享密钥传送给接收方，相应的接收方对随机数进行简单的运算，再使用共享秘钥加密运算后的结果返还给节点 A，这就说明接收方知道这个随机值，同时也保证了发送消息的新鲜性。

5)轻量级

普通的椭圆曲线签名算法中签名需要使用逆运算，而本文所提出的算法所有的运算都是数乘和加减法运算，逆运算的减少可以提高签名和验证的计算量，再者通过采用将签名的预计算（自然地将签名分解出一些可以提前计算的部分），使得在线加密消耗较少的资源，提高在线加密的效率，从而提高系统速度，使得本文的方案轻量化，更适应计算能力有限的体域网节点。

## 4 效能比较

由相关文献可知，计算素数域椭圆曲线上的点加需要 1 个求逆运算，1 个平方运算，2 个乘法运算[10]，这里分别用符号 M、S 和 I 来表示有限域 $GF(p)$ 中的乘法运算、平方运算和求逆运算的计算量，那么点加运算量即 I+2M+S，其中常系数同域元素的乘法计算开销可以忽略不计。假设在仿射坐标系下，表 1 总结了有限域 $GF(p)$ 上相关运算的计算量[11]。

表 1 有限域 $GF(p)$ 上相关运算的计算量

| 运算 | 计算量 |
|---|---|
| 点加运算 | I+2M+S |
| 二倍乘运算 | I+2M+2S |
| 三倍乘运算 | I+7M+4S |

现在对在线/离线椭圆曲线签名和椭圆曲线签名作一个比较，有了以上对于不同运算所产生的不同计算量的考量，这里主要考虑两者在运算方式上的差异，如表 2 所示，分别统计了两种签名系统的运算方式。表中 5、2、1、4 分别指对应签名方案中签名方程和验证方程所包含的该运算方式的次数。

表 2 比较在线/离线椭圆曲线签名

| 运算方式 | 椭圆曲线签名 | 在线\离线椭圆签名 |
|---|---|---|
| 数乘运算 | 5 | 5 |
| 求和运算 | 2 | 4 |
| 求逆运算 | 1 | 0 |

通过对表中数据的分析，可以很清楚地知道，本文所提的方案和原基础的椭圆曲线签名方案均含有 5 次数乘运算，不同的在于本文的方案中不需要求逆运算，只是相应地多了 2 次点加运算，而根据 Brown 等人[12]的粗略估计，求逆运算与乘法运算（带快速取模运算）的开销比是 80:1，求和运算的开销是运算当中最小的相比于求逆运算可以忽略不计，因此用不需要求逆运算的在线\离线椭圆曲线签名方案，存在强大的计算优势。

同时在未确定加密消息之前先做离线加密计算，确定加密的消息和身份公钥后再做在线加密计算，使得在线阶段消耗较少的资源，同时离线阶段进行完计算就可以释放内存资源，这种方案对于计算能力有限的体域网而言是非常有用的。

## 5 结束语

本文通过分析椭圆曲线签名方案的流程，研究了该方案所

存在的问题，包括接收方否认和存在求逆运算使得运算量偏大。针对以上所存在的问题，提出了一种新的在线/离线椭圆曲线签名方案，并对该方案签名流程进行了详细的描述。最后对所提的改进签名方案进行了安全性分析，证明了该方案具有不可伪造、不可否认、抵御重放攻击、轻量级的优点，同时和传统的椭圆曲线签名方案进行了运算量的对比，表明本文所提出的在线\离线椭圆曲线签名方案由于取消了求逆运算，存在强大的计算优势，更适合于体域网的应用。

## 参考文献：


[1] Barakah D M, Ammad-Uddin M. A Survey of challenges and applications of wireless body area network (WBAN) and role of a virtual doctor server in existing architecture [C]// Proc of the 3rd International Conference on Intelligent Systems, Modelling and Simulation. Kota Kinabalu, Malaysia: IEEE Press, 2012: 214-219.

[2] Johnson D, Menezes A, Vanstone S. The elliptic curve digital signature algorithm (ECDSA) [J]. International Journal of Information Security, 2001, 1 (1): 36-63.

[3] Rivest R L, Hellman M E, Anderson J C, *et al.* Responses to NIST's proposal [J]. Communications of the ACM, 1992, 35 (7): 41-54.

[4] Caelli W J, Dawson E P, Rea S A. PKI, elliptic curve cryptography, and digital signatures [J]. Computers & Security, 1999, 18 (1): 47-66.

[5] Tzeng S F, Hwang M S. Digital signature with message recovery and its variants based on elliptic curve discrete logarithm problem [J]. Computer Standards & Interfaces, 2004, 26 (2): 61-71.

[6] 何向军，苏斌. 高效椭圆曲线密码芯片的 VLSI 设计 [J]. 计算机工程，2006, 32 (18): 246-247. (He Xiangjun, Su Bin. VLSI design of efficient elliptic curve cryptography chip [J]. Computer Engineering, 2006, 32 (18): 246-247. )

[7] Ernst M, Henhapl B, Klupsch S, *et al.* FPGA based hardware acceleration for elliptic curve public key cryptosystems [J]. Journal of Systems & Software, 2004, 70 (3): 299-313.

[8] Khalique A, Singh K, Sood S. Implementation of elliptic curve digital signature algorithm [J]. International Journal of Computer Applications, 2010, 2 (2): 21-27.

[9] 陈志德，黄欣沂，许力. 身份认证安全协议理论与应用 [M]. 北京：电子工业出版社，2015. (Chen Zhide, Huang Xinyi, Xu Li. Theory and application of identity authentication security protocol [M]. Beijing: Electronic Industry Press, 2015. )

[10] Kobayashi T, Aoki K, Imai H. Efficient algorithms for tate pairing [J]. IEICE Trans on Fundamentals of Electronics Communications & Computer Sciences, 2006, E89-A (1): 134-143.

[11] Zhao C A, Zhang F G, Huang J W. Efficient Tate pairing computation using double-base chains [J]. Science China: Information Sciences: English Version, 2008, 51 (8): 1096-1105.

[12] Brown M, Hankerson D, López J, *et al.* Software implementation of the NIST elliptic curves over prime fields [C]// Proc of Conference on Topics in Cryptology: the Cryptographer's Track at Rsa. 2001: 250-265.